Smart Contracts on trusted pollution registers

A proposal using Iot devices, Trusted Execution Environments and Blockchain Oracles

Contratos Inteligentes sobre registros confiables de polución

Una propuesta usando dispositivos IoT, entornos de ejecución seguro y oráculos blockchain

Trabajo Fin de Máster

Autor
Angel Algovia García

Dirigido por
Juan Pavón Mestras

Colaborador
Antonio Tenorio Fornés

Convocatoria junio - julio
Calificación 6

Máster Internet de las Cosas
Facultad de Informática
Universidad Complutense de Madrid
2018/2019

por Angel Algovia García

Este documento está preparado para ser impreso a doble cara.

Smart Contracts on trusted pollution registers

A proposal using Iot devices, Trusted Execution Environments and Blockchain Oracles

Contratos Inteligentes sobre registros confiables de polución

Una propuesta usando dispositivos IoT, entornos de ejecución seguro y oráculos blockchain

Trabajo Fin de Máster

Autor
Angel Algovia García

Dirigido por
Juan Pavón Mestras

Colaborador
Antonio Tenorio Fornés

Convocatoria junio - julio
Calificación 6

Máster Internet de las Cosas
Facultad de Informática
Universidad Complutense de Madrid
2018/2019

AngelAlgovia García

El abajo firmante, matriculado en el Máster el Internet de las Cosas de la Facultad de Informática, autoriza a la Universidad Complutense de Madrid (UCM) a difundir y utilizar con fines académicos, no comerciales y mencionando expresamente a su autor el presente Trabajo Fin de Máster: “Contratos Inteligentes sobre registros confiables del Internet de las Cosas”, realizado durante el curso académico 2018-2019 bajo la dirección de Juan Pavón y la colaboración de Antonio Tenorio en el Departamento de Ingeniería del Software e Inteligencia Artificial, y a la Biblioteca de la UCM a depositarlo en el Archivo Institucional E-Prints Complutense con el objeto de incrementar la difusión, uso e impacto del trabajo en internet y garantizar su preservación y acceso a largo plazo.

Director	Colaborador	Autor
D. Juan Pavón Mestras	D. Antonio Tenorio Fornés	Ángel Algovia García

A Jesús y María, mis abuelos,
no pasa un día sin acordarme de vosotros.
A German y Mercedes, mis padres,
que lo han dado todo por mí.

Os quiero.

Agradecimientos

“Andy Dufresne, who crawled through a river
of shit and came out clean on the other side.”
Ellis Boyd 'Red' Redding, The shawshank redemption

Me gustaría agradecer a D. Juan Pavón Mestras y al Grupo de Investigación GRASIA todo el apoyo, paciencia y buenos consejos que han permitido llevar este proyecto a buen puerto.

A Jordi Burguet Castell que admite como idioma materno el lenguaje C, a David Llop Vila un auténtico criptomago, a Viktor Jacynycz García creador de cartera millonarias en segundos y muy especialmente a Antonio Tenorio Fornés por su paciencia y dedicación.

Os estoy realmente agradecido.

Habéis sido brújula en mi océano y viento en mis velas.

¡Gracias!

Resumen

“El mundo hay que fabricárselo uno mismo, hay que crear peldaños que te suban, que te saquen del pozo. Hay que inventar la vida porque acaba siendo verdad.”
Ana María Matute

La contaminación atmosférica se ha convertido en uno de los principales problemas en el cambio climático por la generación de gases de efecto invernadero (GEI) debido a la quema de combustibles fósiles por parte del hombre.

Actualmente no contamos con mecanismos que nos permitan conocer, en tiempo real, la cantidad de dióxido de carbono (CO_2) que expulsa a la atmósfera cualquier fuente de emisión como pueden ser centrales termoeléctricas, la industria o medios de transporte como el marítimo, considerado uno de las fuentes principales de emisión de CO_2.

Tenemos por objetivo la creación de un oráculo descentralizado que permita la adquisición de datos del mundo real a través de dispositivos seguros en el internet de las cosas (IoT), sin la necesidad de ceder confianza a terceros y permitiendo a cualquier actor interesado verificar la autenticidad de los datos generados y hacer uso de ellos.

Este trabajo propone el uso de dispositivos seguros en el internet de las cosas que permitan medir estas emisiones en tiempo real y el uso de las redes blockchain como almacenamiento distribuido de los mismos, permitiendo la adquisición de estos datos por parte de los usuarios de manera gratuita.

Garantizando que los datos se almacenan, procesan y protegen en un entorno aislado y confiable mediante el uso de entornos de ejecución seguro (TEE). Permitiendo la creación de un ecosistema de aplicaciones que ayude a la regulación de la polución e impulse una economía más centrada en la huella ecológica que en el beneficio económico.

PALABRAS CLAVE

Cadena de Bloques, Contrato Inteligente, Oráculo, Entorno de Ejecución Seguro, Dispositivos Confiables del Internet de las Cosas.

Abstract

“El mundo hay que fabricárselo uno mismo, hay que crear peldaños que te suban, que te saquen del pozo. Hay que inventar la vida porque acaba siendo verdad.”
Ana María Matute

Air pollution has become one of the main problems in climate change due to the generation of greenhouse gases (GHG) due to the burning of fossil fuels by man.

Currently we do not have mechanisms that allow us to know, in real time, the amount of carbon dioxide (CO2) that emitted into the atmosphere any source of emissions such as thermoelectric plants, industry or means of transport such as shipping, considered one of the main sources of CO2 emissions.

We aim to create a decentralized oracle that allows the acquisition of real-world data through secure devices in the Internet of Things (IoT), without the need to give confidence to third parties and allowing any interested actor to verify the authenticity of the data generated and make use of them.

This work proposes the use of secure devices on the Internet of things that allow to measure these emissions in real time and the use of blockchain networks as distributed storage of them, allowing the acquisition of this data by users for free .

Ensuring that data is stored, processed and protected in an isolated and reliable environment through the use of secure execution environments (TEE). Allowing the creation of an ecosystem of applications that helps the regulation of pollution and promotes an economy more focused on the ecological footprint than on the economic benefit.

KEY WORDS

Blockchain, Smart Contract, Oracle, Trusted Execution Environment, Trusted Internet of Things Devices.

Índice de contenido

Índice de Imágenes

Consideraciones previas

"La vida cobra sentido cuando se hace de ella
una aspiración a no renunciar a nada"
José Ortega y Gasset

La presente memoria introducirá al lector en las circunstancias en las que ha surgido este proyecto, estableciendo un contexto de las áreas a las que pretende afectar.

Consiste en una introducción que motiva el caso de estudio y la enumeración de los objetivos establecidos para el mismo, así como la tecnología que los sustentan, describiendo las metodologías usadas en la búsqueda de una solución válida.

A continuación se procederá a describir la plataforma de forma incremental. Primero, ofrecemos un resumen de alto nivel del comportamiento diseñado para la plataforma. Después, se describe la implementación con detalles técnicos y de implementación.

Finalmente, se ofrece una conclusión y se establecen varias formas de trabajo futuro.

Introducción

“Let them riso to the challenge of Sustainable Development Goals and act,
not out of self interest, but out of common interest
.I am very aware of the preciousness of time. Seize the moment, act now.”
Stephen Hawking

Este proyecto comparte el espíritu y las motivaciones del grupo de investigación **GRASIA** y su proyecto **P2P Models**[1] en la construcción de organizaciones descentralizadas y democráticas usando tecnología Blockchain, con el fin de impulsar un nuevo tipo de economía colaborativa sostenible. Así mismo el trabajo está en sintonía con los Objetivos para el Desarrollo Sostenible (ODS) de la Organización de las Naciones Unidas (ONU)[2].

El uso de las redes Blockchain y de Smart Contracts proporciona características deseables, como la descentralización de la infraestructura o la posibilidad de crear registros inmutable y transparente.

Sin embargo cuenta con retos importantes, como la incapacidad de obtener datos externos a la Blockchain, para lo que se usa tradicionalmente Oráculos.

Este trabajo propone el uso de las redes Blockchain como almacenamiento distribuido y descentralizado de datos generados por sensores IoT y su acceso por parte de cualquier usuario, aplicándolo a uno de los grandes problemas globales, el cámbio climático.

La contaminación atmosférica se ha convertido en uno de los principales problemas en el cambio climático por la generación de gases de efecto invernadero (GEI) debido a la quema de combustibles fósiles por parte del hombre.

Actualmente no contamos con mecanismos que nos permitan conocer, en tiempo real, la cantidad de Dióxido de Carbono (CO_2) que expulsa a la atmósfera cualquier fuente de emisión como pueden ser centrales termoeléctricas, la industria o medios de transporte como el marítimo, considerado uno de las fuentes principales de emisión de CO_2.

Para ello planteamos la creación de un oráculo descentralizado, que permita la adquisición de datos provenientes de sensores IoT destinados a la medición de emisiones de dióxido de carbono, sin necesidad de entidades intermediarias.

La adquisición de los datos de los sensores se realizará desde entornos de ejecución seguro garantizando que han sido almacenados, procesados en un entorno aislado y confiable.

Los datos generados quedan registrados en la blockchain a disposición de cualquier usuario, permitíendo verificar la veracidad del dato consultado a través del sellado de claves generado por el TEE.

Esto permitirá la creación de un ecosistema de aplicaciones que ayude a la regulación de la polución e impulse una economía más centrada en la huella ecológica que en el beneficio económico.

Objetivos

“Never argue with an idiot. They will drag you down to their level and beat you with experience.”
Mark Twain

Objetivo 1: generación de datos a través de dispositivos seguros en el internet de las cosas para ser suministrados a contratos inteligentes desplegados en la Blockchain.

Actualmente no hay forma de proveer los datos generados por sensores IoT a una Blockchain sin la posibilidad de tener que ceder parte de la confianza en terceros.

Simularemos datos generados por sensores conectados a TEE, que sirva como Oráculo proveedor de datos a redes Blockchain para que puedan para ser utilizado por Smart Contracts desplegados en ella.

Para ello nos basamos en el diseño del proyecto TownCrier de Ari Jules, que conecta de forma segura la información proveniente de Web API's con la Blockchain, para adaptarlo a nuestro propósito en la conexión de sensores IoT directamente a la Blockchain.

Objetivo 2: mejorar la tecnología Blockchain mediante la creación de un Oráculo descentralizado que permita la medición de CO_2 en barcos mercantes.

Como caso de estudio concreto proponemos el diseño de un Oráculo descentralizado que permita la medición de emisiones de CO_2 de buques mercantes, proveyendo de manera segura la información necesaria para interactuar interactuar con aplicaciones externas garantizando la autenticidad de los datos suministrados por sus sensores.

Objetivo 3: generar un ecosistema de Smart Contracts y aplicaciones sobre registros confiables generados por dispositivos IoT seguros.

Mostraremos cómo la aplicación de este concepto puede suponer la creación de un nuevo ecosistema, que permita dar solución a diferentes problema a través de estos nuevos instrumentos tecnológicos, siendo fundamentales en el desarrollo de la sociedad por su gran impacto sobre ella. Como la aplicación de penalización en caso de detectar anomalías o fraudes, la aplicación de legislación de manera inmediata y automática, así como la posibilidad de destinar parte de los beneficios a proyectos ecológicos que los propios usuarios de la red de manera democrática consideren oportunos.

Fundamentos Tecnológicos

Blockchain

"Any sufficiently advanced technology
is indistinguishable from magic."
Arthur C Clarke

En 2008, bajo el pseudónimo de Satoshi Nakamoto se creó un protocolo fiable peer-to-peer como sistema de pago electrónico directo permitiendo, mediante normas, acordar el contenido de los registros sin necesidad de coordinación por terceros.

Este protocolo aloja registros distribuidos e inmutables, denominadas cadenas de bloques o Blockchain, de acceso público y no cifrado[3].

Figura 1 - Cadena de Bloques Blockchain

Se trata de un protocolo robusto ya que, por sus cualidades criptográficas, impide que las cadenas de bloque puedan ser manipuladas; y su información se encuentra replicada en cada nodo de la red, permitiendo verificar su validez por el consenso colaborativo de los usuarios, promoviendo la transparencia.

Por el contrario ofrecen poca usabilidad, una alta volatilidad en los precios de sus criptomonedas y dificultad a la hora de gestionar los errores software. Además, la pérdida o sustracción de las claves de acceso pueden suponer pérdidas millonarias.

La Blockchain no podría dar sentido al acceso aleatorio de información en la cadena al no ser datos secuenciales, otorgándole inmutabilidad.

Estas cualidades le han servido como sistema alternativo a la banca convencional centralizada y privada mediante el uso de las criptomonedas[4]. Como veremos en secciones posteriores, el uso de Blockchain no se limita a las criptomonedas.

Smart Contracts

"The first part of the party of the first part
shall be known in this contract as the first part of the party
of the first part shall be known in this contract"
Groucho Marx

Los contratos convencionales realizan transacciones en función de los niveles de confianza de las partes implicadas. Se requiere de intermediarios, garantías y avales para asegurar su cumplimiento y es subjetiva a interpretaciones pese a su complicada y detallada redacción.

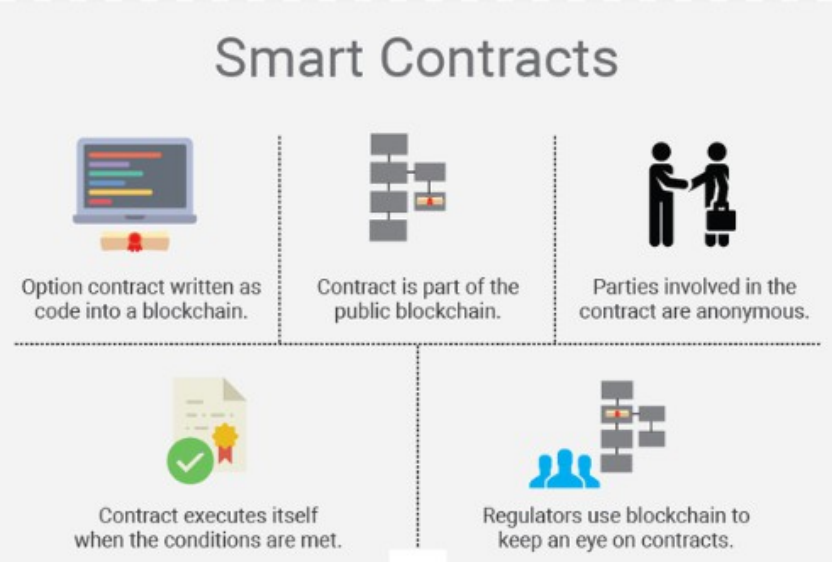

Figura 2 - Smart Contracts, Fuente: //codebrahma.com

Los Smart Contracts (SC), al igual que los contratos convencionales, están diseñados para proveer servicios o bienes a cambio de valores. Son fragmentos de código simple y efectivo que forma parte de la Blockchain y que son ejecutados por los nodos que los mantienen. Se encuentran distribuidos en miles de nodos por eso son públicos, no pueden modificarse y se ejecutan de forma descentralizada, lo cual le da ese carácter inmutable y transparente.

El resultado es un programa auditado por los participantes de la red, que siempre va a actuar de la misma forma sin requerir o depender de la voluntad de terceros[5].

Sin embargo, dado que se basan en redes Blockchain, la información que se transfiere debe ser limitada para no sobrecargar las transacciones ya que almacenar datos en la Blockchain es costoso.

Los contratos convencionales pueden ser creados y llamados por personas al igual que los Smart Contracts, pero estos últimos también pueden ser creados por máquinas u otros programas que funcionan de manera autónoma siendo capaces de ejecutarse y hacerse cumplir por sí mismo, sin intermediarios ni mediadores.

Debido a su naturaleza tienen validez sin depender de autoridades y son accesibles para

todos en la red[6]. Por ejemplo, un Smart Contract que gestiona una cuenta colectiva de un grupo de personas, en la que es necesaria la firma de dos de ellos para poder realizar cualquier transacción monetaria.

Una de las grandes cualidades es que no son interpretables por humanos, son normas establecidas por código que evitan interpretaciones subjetivas y el no cumplimiento por parte de las partes. Elimina intermediarios que lo validen o que garanticen su cumplimiento, ahorrando costes al consumidor y trasladando la confianza a un entorno de ejecución determinista. Por el contrario pueden tener importantes errores de código que ya no son reparables, pudiendo llegar a ser imparables.

Oráculos

"Technology is a useful servant but a dangerous master."
Christian Lous Lange

Los Oráculos son servicios confiables que envían información a los Smart Contracts aliviando la carga de trabajo a la Blockchain. Proporcionan los datos necesarios para desencadenar la ejecución de Contratos Inteligentes cuando se cumplan los términos establecidos. Funcionan como traductores para facilitar información a plataformas externas como Oraclize que provee a Smart Contracts provenientes de WebAPI y Dapps[7].

Por ejemplo, el proyecto TownCrier proporciona información sobre vuelos retrasados provenientes de la WebAPI de una aerolínea. Esta información podría servir para realizar un sistema de reembolso automático ante retrasos, mediante un Smart Contract en la Blockchain.

Un Smart Contract no puede interactuar con el mundo exterior a la Blockchain y aunque quisiera no podría acceder a información fuera de la red. Cuando los datos llegan a Blockchain desde un Oráculo, la información se usa para ejecutar los Smart Contracts permitiendo intervenir en los casos de uso de la industria en general[8].

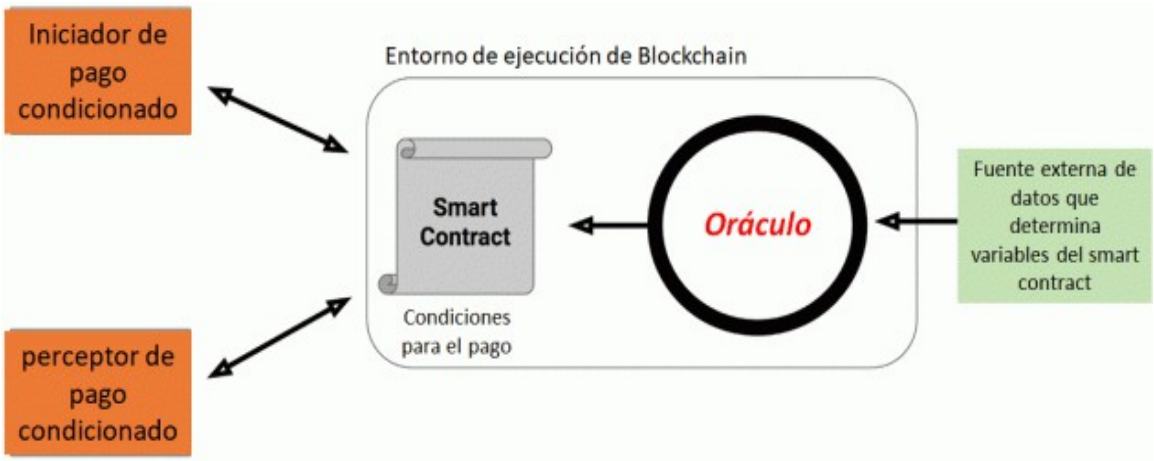

Figura 3 – Diagrama componentes de un oráculo

Los Smart Contracts y la Blockchain en sí se caracterizan por ser descentralizados, por el contrario los Oráculos son proveídos por terceros y autorizados por las compañías privadas que los utilizan, lo cual crea un obstáculo en el debate de la cesión de confianza en terceros[9]. Por ese motivo es objetivo de este Trabajo Fin de Máster proporcionar un Oráculo descentralizado que ofrezca información a la Blockchain sin confiar en terceros.

Entornos de Ejecución Seguros

"The great growling engine of change. - Technology"
Alvin Toffler

Un Entorno de Ejecución Seguro (TEE – Trusted Execution Environment) es un área segura del procesador principal de un dispositivo conectado que garantiza que los datos confidenciales se almacenan, procesan y protegen en un entorno aislado y confiable.

Está preparado para el desarrollo de aplicaciones que buscan impedir la divulgación o la modificación de ciertos códigos y datos por medio del uso de enclaves, que son áreas de ejecución protegidas en la memoria.

El propósito es brindar seguridad de extremo a extremo al proteger la ejecución de código, la integridad del Sistema Operativo y BIOS incluso en presencia de malware privilegiado, los derechos de acceso a la plataforma y la veracidad de sus datos mediante autentificación remota, utilizando mecanismos basados en hardware para responder a problemas que validan su integridad[10].

Por ejemplo, Microsoft Azure Confidential Computing ahora presenta seguridad basada en hardware con Intel SGX, permitiéndole proteger los datos no solo en el envío de información, sino también cuando está en uso en la memoria.

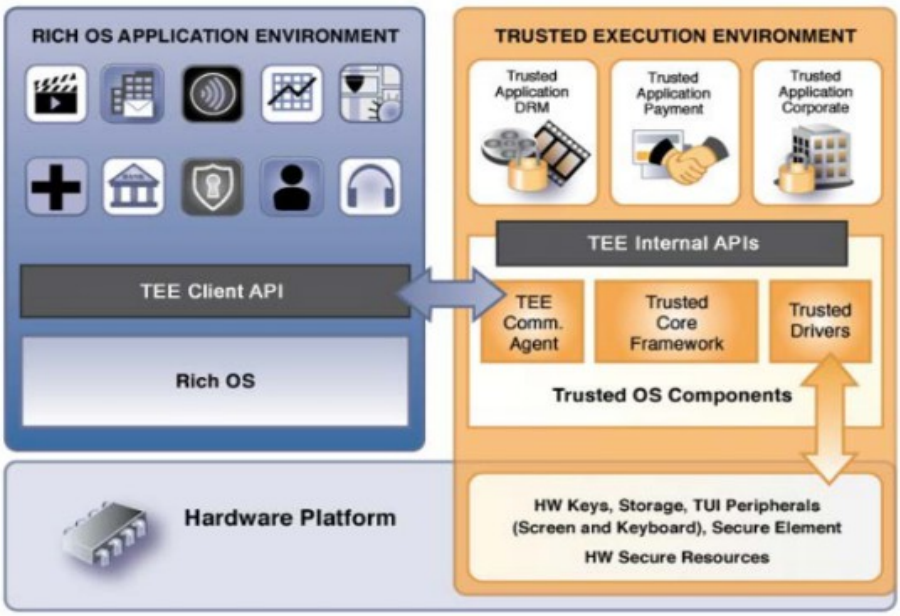

Figura 4 -Trusted Execution Environment, Fuente://accourt.com

El objetivo de la atestación remota asimétrica es que una entidad genere confianza como proveedor de servicios, proporcionando los secretos solicitados y verificando tres cosas: la identidad de la aplicación, su integridad (que no ha sido manipulada) y que se está ejecutando dentro de un enclave.

Como resultado se produce una clave que se puede usar para cifrar los secretos en el enclave y descifrarlos por otras aplicaciones sin necesidad de tener hardware habilitado

TEE.

El protocolo de atestación remota prueba que una pieza específica de código se ejecutó en un hardware adecuado, produciendo un resultado específico. El mensaje final que completa el protocolo es una declaración firmada, llamada cotización, que contiene el certificado de firmas.

Un informe de verificación positivo confirma que el enclave ejecuta un fragmento de código particular en un procesador genuino generando una respuesta adecuada a la plataforma del otro extremo[11].

Dispositivos IoT Seguros

"If you think technology can solve your security problems,
then you don't understand the problems and
you don't understand the technology."
Arthur C Clarke

La seguridad en IoT, y en sus dispositivos, es un proceso continuo que debe tenerse en cuenta en todas las fases del ciclo de vida software involucrando a todos aquellos que participan en la gestión, uso, aseguramiento y fabricación. Esto permite alargar la vida útil de nuestros dispositivos y su correcto funcionamiento, evitando así problemas de ciberseguridad que no solo afectan a nuestro dispositivo, sino que puedan expandirse hasta llegar a otros[12].

Dentro de la amplia variedad de dispositivos que pueden ser conectados a IoT se establecen una serie de procedimientos que favorecen la seguridad de los dispositivos conectados. Es recomendable revisar las especificaciones de seguridad de cada uno de los dispositivos, estableciendo un plan de reemplazo si el ciclo de vida de un dispositivo finalizó.

Para favorecer la creación de dispositivos seguros es necesario que sean actualizados de manera regular con la última versión del software, ya sea sistema operativo o firmware, evitando así vulnerabilidades detectadas por el fabricante.

Es conveniente el uso de las medidas implantadas en el dispositivo para autenticación y control de accesos, obligando al uso de contraseñas seguras y evitando accesos no deseados.

Es conveniente que los datos generados por los dispositivos IoT guardados de forma segura con un cifrado contundente, concretando dónde se almacenan y el tipo de información que almacena. En caso de ser gestionado desde la nube será necesario establecer una conexión cifrada mediante el uso de protocolos seguros[13].

Estado del Arte

"Never spend your money before you have it."
Thomas Jefferson

El uso de las redes Blockchain y de Smart Contracts proporciona características deseables, como la descentralización de la infraestructura o la posibilidad de crear registros inmutable y transparente. Actualmente ya podemos encontrar organizaciones y herramientas que permiten a la Blockchain interactuar con el mundo real a través de oráculos.

Los oráculos, en contraposición con el espíritu Blockchain, suelen ser provistos por empresas privadas, como la empresa SmartContract (no confundir con el concepto Smart Contracts) que pretende ser un Oráculo entre la banca convencional y la Blockchain.

La empresa Oraclize crea conexiones entre la Blockchain y Web API's o Dapps, perdiendo la capacidad de descentralización y transparencia al ser mantenidos por una sola entidad centralizada y no ser sostenidos y supervisados por sus contribuidores.

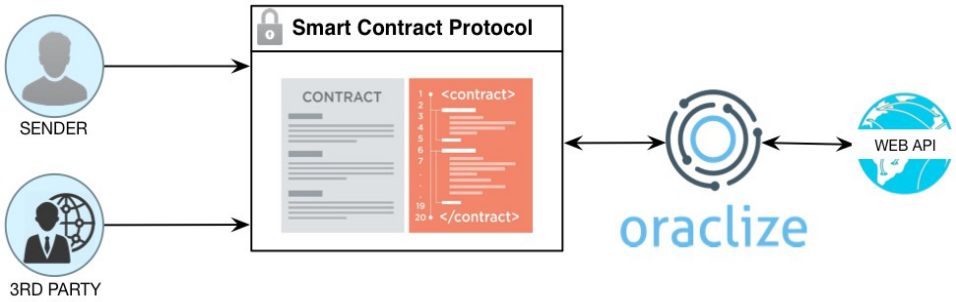

Figura 5 - Diagrama oraclize

En la línea de creación de Oráculos descentralizados podemos encontrar a ChainLink que intenta crear la primera red de Oráculos que permita a los Smart Contracts conectarse a feeds de datos externos, así como a APIs o sistemas de pago.

El proyecto Town-Crier de Ari Jules, un Oráculo que aprovecha la potencia del TEE de Intel SGX para garantizar la procedencia e integridad de la ejecución de código que permita interactuar con Smart Contracts.

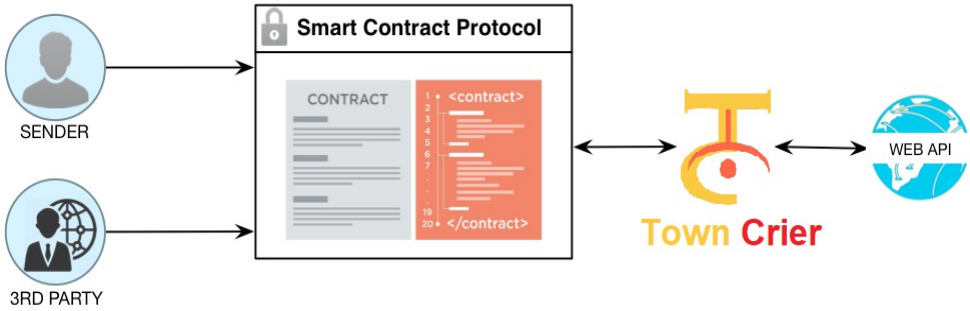

Figura 6 – Diagrama Town-Crier

Lo interesante de nuestro estudio es el hecho de no tener que ceder esa confianza Oráculos pertenecientes a empresas privadas o Web API's que no sabemos de qué forma hacen la adquisición de esos datos. Proponiendo conectar directamente los sensores a un Entorno de Ejecución Seguro que ofrezca a la Blockchain un registro confiable de datos, pudiendo verificar la integridad de los mismos.

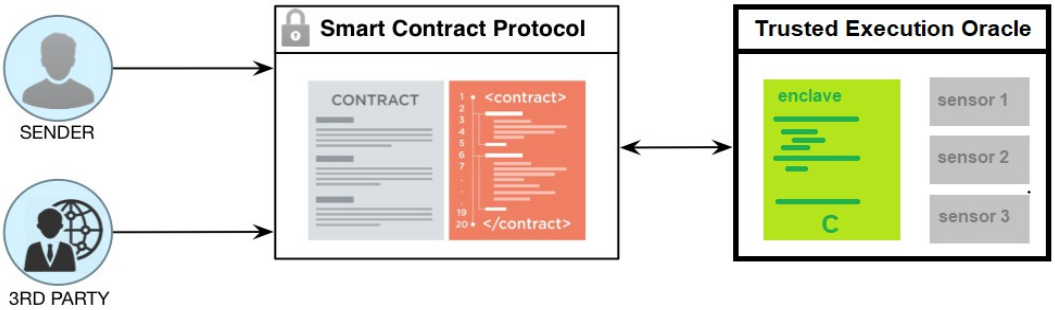

Figura 7 – Diagrama Trusted Execution Oracle

Metodología de Trabajo

"En principio la investigación necesita más cabezas que medios."
Severo Ochoa

El presente Trabajo Fin de Máster (TFM) es un proyecto de desarrollo encaminado a resolver un problema real, con una casuística particular y sin conocimientos previos del entorno de trabajo.

Por su naturaleza se trata de una investigación explorativa en la que para evitar perdernos en el aparente caos de los fenómenos nos basamos en lecturas de textos científicos-tecnológicos y en la consulta a expertos en el sector para la generación del conocimiento necesario y no caer en planteamientos erróneos del problema[14]; cualitativa, al buscar analizar el problema mediante sus procesos y resultados; descriptiva, al tener poca información del fenómeno y cuyo conocimiento de las propiedades determinadas permite dar explicaciones a otros asuntos que guardan relación[15]; explicativa, estableciendo una relación causa-efecto que permite la formulación de leyes y normas; y evaluativa analizando la eficiencia, eficacia, efectividad e impacto social del proyecto.

"La evaluación es el proceso de identificar, obtener y proporcionar información útil y descriptiva acerca del valor y el mérito de las metas, la planificación, la realización y el impacto de un objeto determinado con el fin de servir de guía para la toma de decisiones, solucionar los problemas de responsabilidad y promover la comprensión de los fenómenos implicados."

D.L.Stufflebeam y A.Schiklield. 1987
Evaluación sistemática. Guía teórica y práctica. Madrid: Paidós/MEC. p. 183.

Se han seguido los principios del "*Manifesto for Agile Software Development*"[16] con la idea de desarrollo evolutivo en el cada ciclo de definición de necesidades, análisis, diseño, codificación, pruebas, validación y evolución nos acercarse más a la solución deseada. Sin embargo no se ha aplicado una metodología ágil en concreto.

La metodología aplicada al proyecto se detalla a continuación:

Identificación y planteamiento del problema

Observando nuestro entorno, viendo las noticias o atendiendo las notificaciones de alerta de alta contaminación en nuestras ciudades podemos identificar entre los grandes problemas de nuestros días la contaminación medioambiental que el hombre produce mediante la quema de combustibles fósiles, emitiendo grandes cantidades de CO_2, esta temática que nos motiva para establecer todas las contradicciones internas con respecto a esta y los factores que la afectan, impactan o modifican, creando así nuestra situación de objeto de estudio.

La sección de motivación de la introducción y la sección Identificación y planteamiento del problema de este trabajo profundizan en estos aspectos.

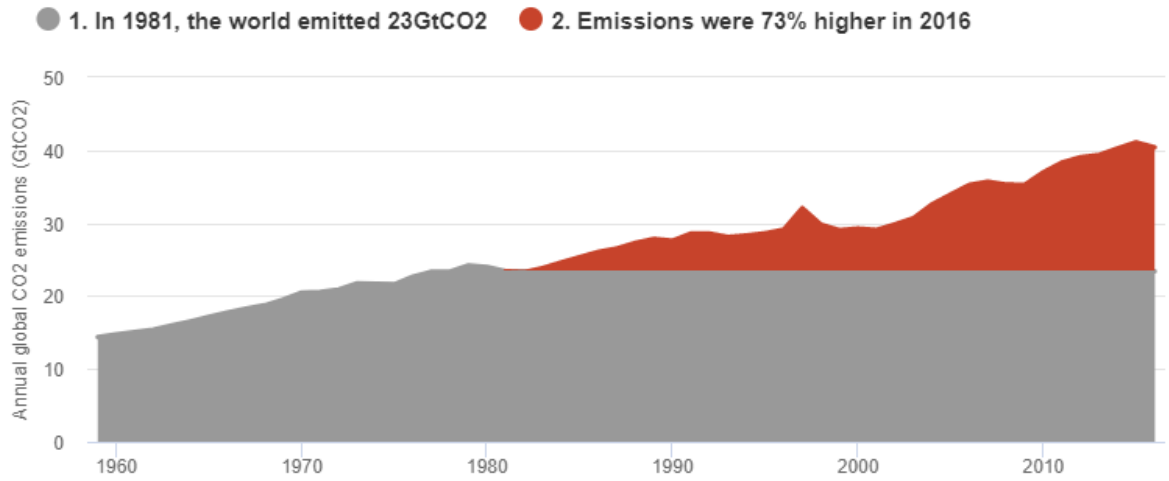

Figura 8 -Global CO2 Emissions 1959 - 2016, Fuente: Carbon Brief

Ponderación de los motivos del problema

La recopilación, análisis y comparación de textos especializados nos permite la exploración de posibles soluciones, determinando las causas probables y la elección de mejores aproximaciones a una solución viable.

Para la correcta ponderación de los motivos del problema se mantuvieron varias reuniones con el objetivo de ampliar esta información, como la organizada por D. José Ignacio Gómez Pérez, profesor de la asignatura “Arquitectura Sobre el Nodo IoT” con la empresa Linked Carbon Hub - Climate Change Advisors encargada de realizar el cálculo de emisiones en buques mercantes en España[17]; la organizada con Wedge Global Rola EI-BIJOU por parte de D. Antonio Tenorio, empresa en el sector de la generación de energías renovables[18]; o los eventos “MeetUp Blockchain 4 Good Rocks”[19], que ayudó a la comprensión de este movimiento democrático y descentralizado, y “Smart Space And Agreements” organizado por FabLab Barcelona para la divulgación IoT.

Diseño

En el campo tecnológico, el planteamiento y la resolución de problemas supone igualmente el desarrollo lógico de un conjunto de fases, de acciones cuya ejecución facilitará la resolución del problema.

En el desarrollo de este proyecto se han desarrollado diferentes prototipos para intentar abarcar el objetivo de este TFM. En la sección de Diseño de este trabajo, se mostrará el diseño final mostrando la arquitectura del sistema, explicaremos por separado cada una de sus partes así como su funcionalidad, mostrando un Diagrama de Secuencia que apoye la explicación del mismo.

Implementación tecnológica

Este TFM pretende ser una prueba de concepto de viabilidad tecnológica de dispositivos seguros en el IoT que usen TEE para garantizar la integridad de los datos y se conecten a una Blockchain para el registro transparente e inmutable de los mismos.

Esto garantiza que los datos se almacenan, procesan y protegen en un entorno aislado y confiable.

Su interés está en la implementación de un prototipo a través de TEE y Smart Contracts, explicando los pasos necesarios para alcanzar los requisitos del sistema que plantemos. Permitiendo realizar las pruebas necesarias de viabilidad. La descripción de la implementación realizada puede encontrarse en la sección Implementación de este trabajo.

Pruebas y análisis de resultados

Las pruebas y posterior análisis de resultados deben mostrar su relación con el diseño, señalando los aspectos no resueltos, sin tratar de ocultarlos y delimitando aquellos resultados con lo que no cuadre.

En este trabajo se ha probado la creación del certificado de firmas de Intel SGX y su uso en la firma de datos simulados por sensores poniéndolos a disposición de la Blockchain. Así como la verificación de la firma generada por Intel SGX en su proceso de Atestación Remota en un Smart Contract que carece de hardware específico Intel SGX.

Conclusiones

Para determinar el grado de cumplimiento de los objetivos propuestos en este proyecto y después de explicar las bases teóricas de la investigación y las posibles aplicaciones prácticas que pueda tener, podemos formular de forma clara y detallada de donde nacen nuestras conclusiones y para qué sirven.

Planteamiento de trabajos futuros

Como en cualquier otro proyecto, durante su desarrollo, han surgido algunas líneas de investigación futuras que se han dejado abiertas y en las que es posible continuar trabajando; algunas de ellas, están más directamente relacionadas con este trabajo de fin de máster y son el resultado de cuestiones que han ido surgiendo durante la realización de la misma. Otras, son líneas más generales que, sin embargo, no son objeto de este proyecto.

Identificación y planteamiento del problema

"Any sufficiently advanced technology
is indistinguishable from magic."
Arthur C Clarke

El martes 8 de diciembre de 1981 el canal de televisión británico ITV emitió el documental llamado “Warning Warning” convirtiéndose en una de las primeras emisiones a nivel mundial dedicado exclusivamente al cambio climático provocado por el hombre[20].

Amplios son los factores con los que el hombre contribuye al cambio climático, pero en la década de los 90 empezamos a familiarizarnos con el término gases de efecto invernadero (GEI) al verse incrementado notablemente debido a la quema de combustibles fósiles principalmente. Treinta años después sabemos que la tasa de crecimiento global de dióxido de carbono, uno de los gases de efecto invernadero, se ha visto cuadruplicado desde la década de los sesenta.

Esto tiene como consecuencia la pérdida de biodiversidad, disminución del agua potable, cambios meteorológicos extremos como olas de frío y calor, sequías e inundaciones, aumento de incendios forestales y un largo etcétera que finalmente termina afectando a la biosfera y a la salud humana. Ante la obviedad del cambio climático debido a estos gases se ha llevado su regulación de diversas maneras.

Como podemos ver en la imagen mostrada a continuación, la IMO prevé un crecimiento de las emisiones de CO_2 en los próximos que pretende reducir aplicando medidas de eficiencia energética . El motivo de este futuro crecimiento se debe principalmente al comercio internacional y la globalización de la economía, al ser este medio de transporte el más económico y fiable.

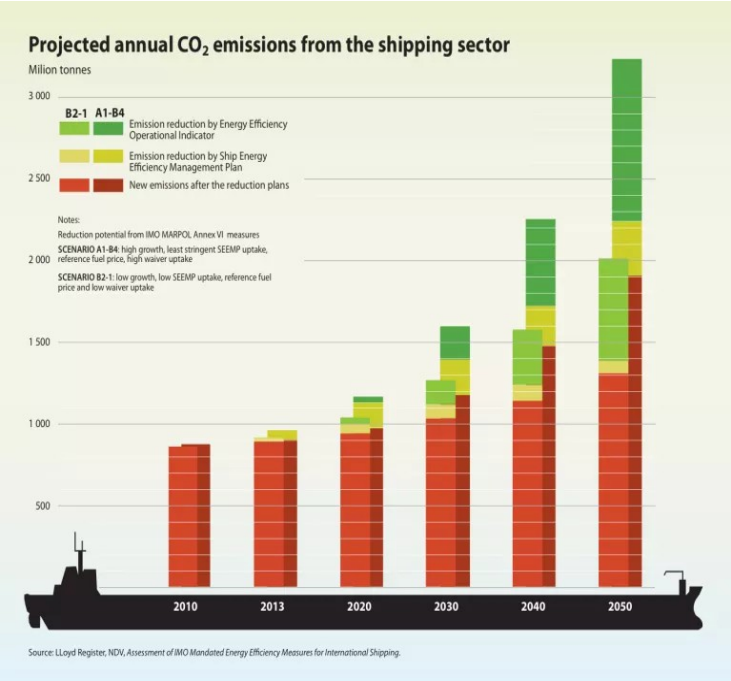

Figura 9 - Previsión emisiones anuales CO2 en el sector marítimo, Fuente: International Maritime Organism

En este sentido el Protocolo de Kyoto reconoce que las emisiones de gases de efecto invernadero provenientes del transporte marítimo no pueden ser atribuidas a ninguna economía nacional en razón de su emisión en aguas internacionales.

La Organización Marítima Internacional (IMO), organismo de las Naciones Unidas encargado de la seguridad y la protección del transporte marítimo, creó el Convenio Internacional MARPOL - ANEXO VI, adoptado en 1997, para determinar las reglas que deben prevenir la contaminación atmosférica ocasionada por los buques de carga.

El convenio determina que todo buque de carga debe ser inspeccionado cada cinco años para certificar que las emisiones son acordes al tipo de motor que usa. Inicialmente no se contaba con mecanismos sancionadores ante la ausencia de tal certificación.

Para el cálculo de emisiones se solicita anualmente a cada buque la entrega de los recibos de combustible para calcular aproximadamente el volumen de emisiones según litros consumidos y tipo de motor. Este sistema puede ser susceptible a fallos y fraude debido a la pérdida o extravío de facturas u omisión de las mismas. La alta latencia en la toma de datos impide conocer las emisiones del buque en una fecha determinada y que el proceso no sea público lo hace poco transparente.

Para la regulación de estos gases la IMO decidió formar parte de los mercados de derechos de emisión, diseñados y organizados por los poderes públicos, como marco de un acuerdo internacional en la regulación económica y medioambiental.

Estos Mercados de Emisiones fueron concebidos con la idea de reducir las emisiones que producen las empresas en su actividad industrial ya que su producción conlleva un coste agregado por contaminación. Se permite que aquellas empresas más ecológicas cuenten con un exceso de bonos otorgados que pueden vender a otra empresa en un mercado libre de emisiones[21].

El propio nombre indica que se trata de la compra venta de bonos de emisión de gases contaminantes. Estos mercados suelen ir regulados por gobiernos o organizaciones internacionales, como podrían ser Estados Unidos o la Unión Europea, que determinan el número de bonos con lo que cuenta una empresa para su actividad industrial, sub dividiéndose en tipos de emisión, lo que hace que sean mercados pequeños y muy localizados e impidiendo la posibilidad de una regulación total de la actividad empresarial a nivel mundial.

La ausencia de emisiones por parte de una empresa lo habilita para ofrecer su exceso de bonos en un mercado libre de emisiones, lo que ha permitido que tan solo en el último año el precio por tonelada se haya visto incrementado en un 200%, pasando de 8 € por tonelada a 24 € y permitiendo que lo que no contamina una empresa lo contamine otra.

Podemos concluir que:

- Existe un exceso de organizaciones nacionales, internacionales, gobiernos, mecanismos reguladores, legislaciones, convenios, normas... que dificulta burocráticamente atajar el verdadero problema, los gases de efecto invernadero.

- La adquisición de datos en el cálculo de emisiones para los Mercados de

Emisiones es lenta y poco fiable. El cálculo de emisiones no es público e impide su verificación por otras partes.

- Son estos problemas, los que motivan la búsqueda de una solución tecnológica que cree un marco de trabajo mundial que no dependa de autoridades, gobiernos o terceras partes y que mejore el cálculo de emisiones.

Ponderación de los motivos del problema

"Any sufficiently advanced technology
is indistinguishable from magic."
Arthur C Clarke

La regulación de GEI mediante los mercados de derechos de emisión se encuentran subdivididas en zonas geográficas y tipos de emisiones dificultando que se tomen medidas globales que atajen y reviertan el efecto invernadero.

La información que proveen los buques para el cálculo de emisiones puede que no sea correcta. La forma de adquisición de datos es lenta e ineficiente al necesitar una recopilación de facturas físicas, caracterizándose por una alta latencia, que impide conocer las emisiones en tiempo real o la acumulación de emisiones en un rango de tiempo.

El proceso que audita las emisiones anualmente no se realiza de manera pública, carece de transparencia, realizándose por empresas privadas al servicio de las organizaciones gubernamentales.

La concesión de bonos por emisión no ha supuesto una reducción de las emisiones ya que el mercado ha empezado a especular con el precio por tonelada emitida.

No existe posibilidad real a día de hoy de saber la cantidad de contaminación emitida por un buque en un periodo de tiempo o en una zona determinada ya que no disponemos de sistemas que nos permitan adquirir el dato de contaminación en tiempo real y asegurar la veracidad de ese dato sin intervención de terceros.

Diseño

"Failure is simply the opportunity to begin again,
this time more intelligently."
Henry Ford

Tenemos por objetivo de diseño la creación de un oráculo descentralizado que permita la adquisición de datos del mundo real a través de dispositivos seguros en el internet de las cosas, sin la necesidad de ceder confianza a terceros y permitiendo a cualquier actor interesado en esta información pueda verificar la autenticidad de los datos generados y hacer uso de ellos.

Sería realmente sencillo el uso de un oráculo tradicional, como Oraclize, para recopilar la información necesaria y regular el SC con esos datos, pero incurriríamos en esa cesión de confianza, ya que desconocemos la forma en que el oráculo recopila y dispone de la información, así como la estructura interna de Oraclize a la hora de atestiguar la veracidad de sus resultados. Esto es algo que nos permitirá resolver el uso de TEE y la Atestación Remota, como propone el proyecto TownCrier.

El presente diseño plantea un sistema para un buque mercante dotado con el dispositivo de medición necesario para calcular el número de litros de combustible consumidos, del cual sabemos su modelo de motor y que se encuentra adscrito al Smart Contracts MARPOL- ANEXO VI es capaz de pagar en los mercados de emisión de CO_2 las emisiones totales realizadas en un año.

El sistema es capaz de resolver el problema específico de la contaminación en buques mercantes y puede ser adaptado para permitir la conexión de otros tipos de sensores IoT conectados a TEE a la Blockchain.

Arquitectura del Sistema

Nuestra sistema de medición y registro confiable de polución en barcos mercantes consta de dos partes claramente separadas por sus entornos de ejecución.

El oráculo (O) descentralizado, provisto desde el dispositivo (D), como set de sensores conectados a un TEE Intel SGX, que sella criptográficamente los datos recopilados por los sensores poniendo la información a disposición de los usuarios; y el Smart Contract (SC), desplegado en la cadena de bloques, que realiza la verificación de la integridad de los datos sellados por Intel SGX.

La entidad EPID de IBM es el servicio de certificación que Intel provee para verificación de la identidad de los microprocesadores Intel SGX mediante la Atestación Remota.

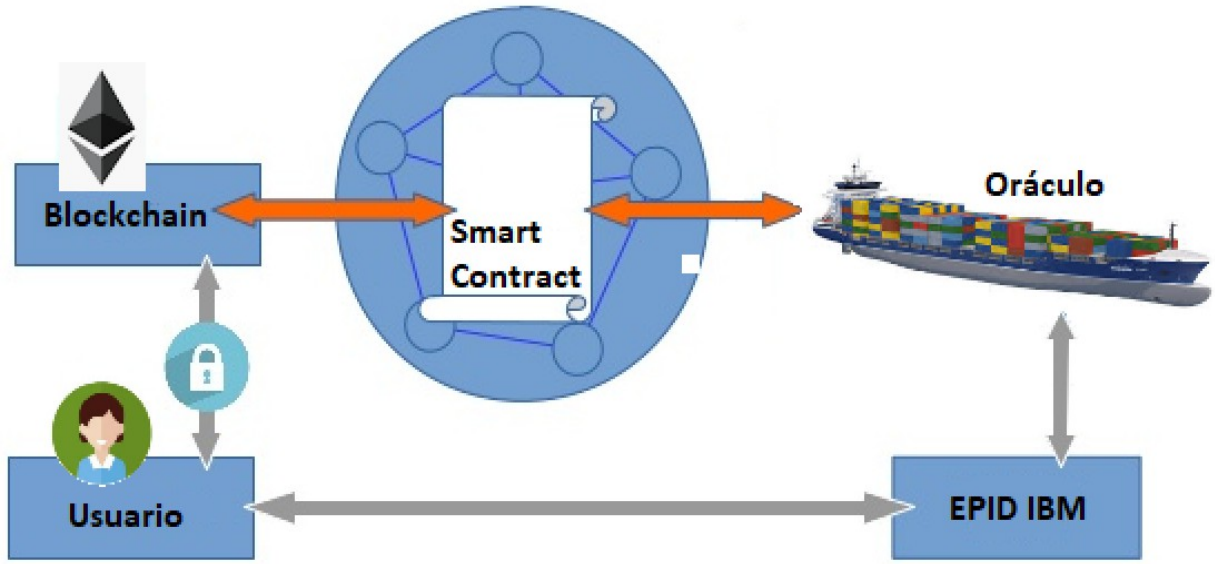

Figura 10 - Diagrama de Componentes del Sistema

El propósito es que el dispositivo realice las funciones de Oráculo descentralizado y que genere confianza como proveedor de servicios en el cálculo de emisiones de CO_2.

Adquiriendo como resultado de su conexión con el EPID IBM (Atestación Remota) una clave que puede ser usada para firmar mensajes y ser verificada en un SC que no cuenta con hardware habilitado para Intel SGX verificando cuatro cosas:

- la identidad del dispositivo,
- su integridad (que no ha sido manipulado),
- que se ejecuta en la última versión firmware y que ejecuta un código concreto,
- y que se está ejecutando dentro de un Enclave Intel SGX.

El SC, siendo visible globalmente en la cadena de bloques y contando con el código necesario para comprobar la firma del Intel SGX, verifica la firma del dato y lo guarda.

Dejándolo a disposición de cualquier usuario interesado en esta información.

Otros tipos de contratos podrían ser autoejecutables, por ejemplo, obligando a las partes a fijar un precio por tonelada de CO_2 emitidas anualmente. Siendo de obligado cumplimiento, esto impediría la especulación en los mercados de emisiones y se pagaría por las emisiones reales y no por la concesión de bonos de emisión.

El contrato también podrá modelar otro tipo de cláusulas como la aplicación de penalización en caso de detectar anomalías o fraudes, así como la posibilidad de destinar parte de los beneficios a proyectos ecológicos que los propios usuarios de la red de manera democrática consideren oportunos.

El usuario bajo estas condiciones dispondrá del dato firmado y su clave pública en la Blockchain, pudiendo comprobar la veracidad del dato sin necesidad de disponer hardware Intel SGX.

También podrá realizar Atestación Remota ante la entidad EPID de IBM en busca de verificación de la identidad del dispositivo, que atestigua que el dato no ha sido manipulado al ejecutarse en la última versión firmware del enclave de un Intel SGX con identidad válida.

Funcionalidad

La interacción entre las diferentes partes presentadas en la arquitectura anterior nos permitirán cumplir la funcionalidad propuesta para este proyecto:

- Registro de la identidad de los sensores de los barcos a través de Smart Contracts proporcionando la clave del TEE.

- La medición y sellado de datos por parte de un TEE que nos asegura que no han sido manipulados, siendo adquiridos directamente de los sensores a los que está conectado.

- Verificación de la firma del TEE en Smart Contracts y otros entornos al no ser necesario software específico Intel SGX.

- El registro de datos verificados en la Blockchain disponibles de primera mano sin necesidad de intermediarios.

- Consulta de los datos registrados por el dispositivo, garantizando que:
  - los datos se han generado en un TEE,
  - que el TEE en el que se ha generado es el del barco,
  - que los datos no han sido manipulados desde que salieron del TEE hasta su entrada en la blockchain, (
  - que los datos que se han registrado en la blockchain están disponibles desde la fecha en la que se registraron y
  - que no se han modificado desde entonces.

- Verificar la validez de la clave del TEE a través de la infraestructura de Intel recibiendo una respuesta de verificación de identidad.

Además en futuras versiones de la herramienta, se podrán automatizar comportamientos derivados de los datos de contaminación registrados: multas por exceso de emisiones, cobros por emisiones reales, sellos de "transporte ecológico" para clientes que busquen una eficiencia energética concreta, etcétera.

La disposición del dato firmado permiten que otro tipo de aplicaciones que hacen uso de la Blockchain puedan adquirirlo sin necesidad de intermediarios, facilitando el desarrollo de un ecosistema de aplicaciones vinculadas a estos datos.

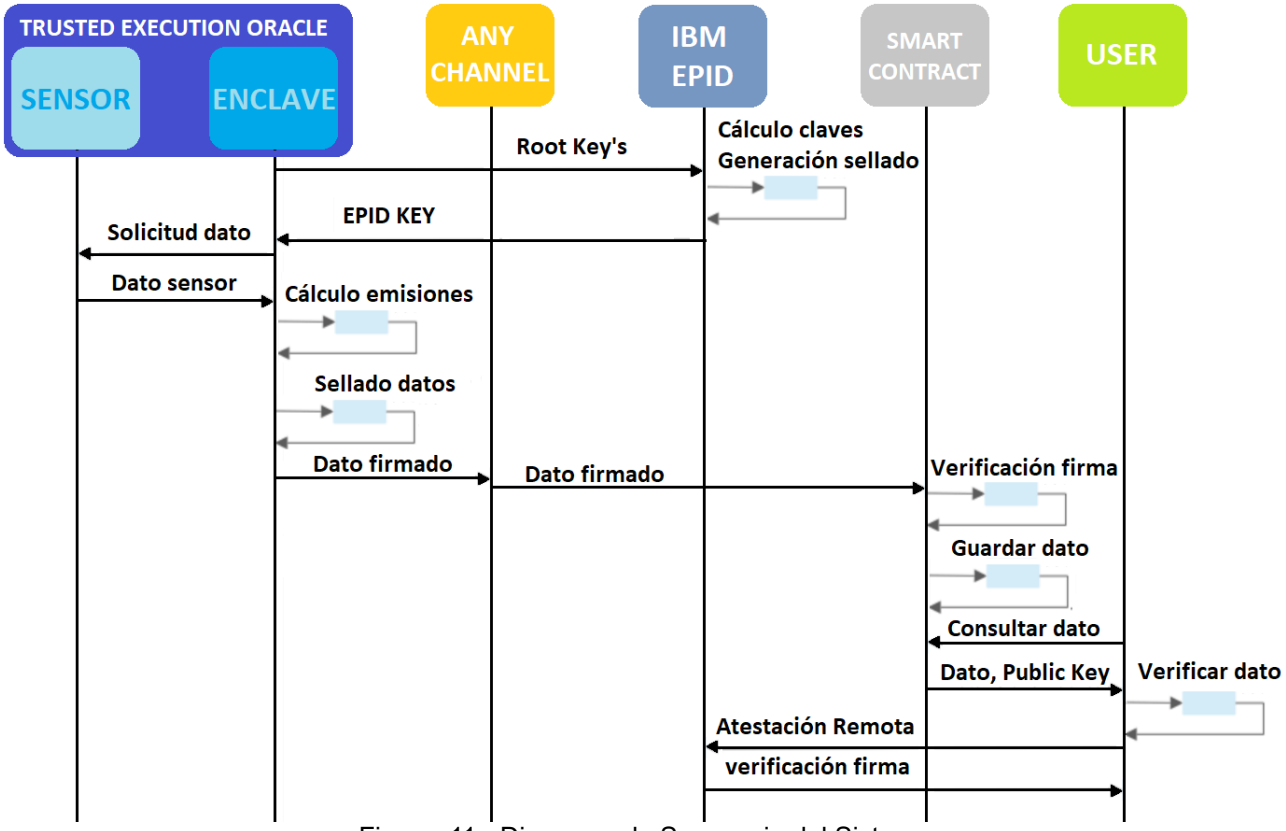

Figura 11 - Diagrama de Secuencia del Sistema

El dispositivo (D)

Dentro de las medidas establecidas para los Dispositivos IoT Seguros, se han establecido una serie de requerimientos de fabricación e instalación englobados en los procesos de seguridad contínua que pasaremos a describir a continuación.

Características Hardware

- El dispositivo contará con un entorno de ejecución seguro Intel SGX conectado a diversos sensores:

    - Sensor RTK de posicionamiento global:

        - Se tratan de sensores más robustos que los conocidos GPS, al tomar la posición global mediante el cálculo de posiciones entre diferentes constelaciones mejorando su exactitud. El objetivo es conocer la posición exacta del buque en todo momento.

- Sensores para medición volumétrica:

    - El objetivo de estos sensores es conocer la cantidad de litros de combustible de los que dispone un buque (indicador de gasolina). Sabemos por la Ley de Gay-Lussac que el volumen guarda relación con la presión y la temperatura por lo que sería lógico poner este tipo de sensores.

- La fabricación del dispositivo será encargado al fabricante IBM, propietario del Intel SGX, con diseño bajo demanda.

    - Se toma esta decisión debido a que IBM garantiza en su gama Intel SGX la creación de claves para identificar que un código o dato ha sido ejecutado en un procesador Intel SGX legítimo, sin que Intel conozca cuál ha sido el resultado de estas claves calculadas, evitando que cualquier empresa u organismo conozca las mismas.

    - Además en el proceso de Atestación Remota Intel no tiene la posibilidad de almacenar el resultado de la firma creada, evitando la cesión de información a terceros.

- El producto debe ser entregado en un encapsulado que garantice que la integridad de los componentes en su interior.

    - Nuestro dispositivo será instalados en entorno donde existirán partículas en suspensión, alta humedad y vibraciones al tratarse de la sala de máquinas de un buque mercante.

    - Como referencia recomendamos como mínimo un encapsulado que evite el polvo y humedad.

    - En este mismo sentido somos conscientes de la Anomalía del Atlántico Sur que provoca variaciones del campo magnético que podría interferir en nuestro sistema, por lo que sería conveniente dotarlo de apantallamiento a este efecto.

- Igualmente el encapsulado debe impedir, en la medida de lo posible, el intento de manipulación física externa.

- Además en necesario que esté dotado para situar un sello o lacre de garantía e instalación correcta en su exterior que impida la apertura del dispositivo.

Microprocesador Intel SGX en el Dispositivo (D)

El Entorno de Ejecución Seguro del Intel SGX es el encargado de generar las firmas de sellado para el envío de mensajes así como ofrecerse como un proveedor de datos seguros que devuelva una respuesta en forma de datagrama que nuestro Smart Contract comprenda al adquirir el resultado de los cálculos realizados con los datos de los sensores para el cálculo de emisiones de CO_2.

El enclave (E), como zona segura de memoria, es la encargada de verificar la identidad de la aplicación, su integridad y su ejecución segura. Para ello realiza el proceso de Atestación Remota contra servidores de IBM que definimos a continuación.

La llamada a los sensores, así como el programa que realiza la función del cálculo de datos debe ejecutarse como una rutina en el Enclave para asegurar la integridad de los datos y usar el certificado de firmas para ser encriptado.

El enclave (E) es una instancia de código ejecutándose en el área de memoria reservada de un Intel SGX, provee la información que necesita el Smart Contract. Para obtener los datos, consulta las mediciones de los sensores conectados al TEE, devolviendo la información como un mensaje firmado.

Bajo nuestro modelo básico de seguridad para SGX, el software de medición y atestación de los datos generados se ejecuta en completo aislamiento, bajo la seguridad del Enclave. Asegurando que la identidad de Intel SGX es correcta y que el código ha sido ejecutado dentro del Enclave evitando posibles manipulaciones.

Además proporciona una clave pública única para la instancia del Enclave al cliente y demuestra que el Enclave está ejecutando correctamente código en un enclave SGX. Permitiendo crear Smart Contracts dependientes del TEE.

Todo esto sirve para atestiguar que la fuente de datos es segura y fiable al no depender de empresas privadas o terceros, que se toma el dato desde los sensores sin entidades intermediarias, y que el dato es firmado y sellado por un entorno de ejecución seguro.

Intel SGX - Atestación Remota

Para poder crear y verificar el certificado de firmas generadas por Intel SGX es necesario realizar un registro en IBM siguiendo un esquema desarrollado por Intel llamado ID de Privacidad Mejorada (EPID).

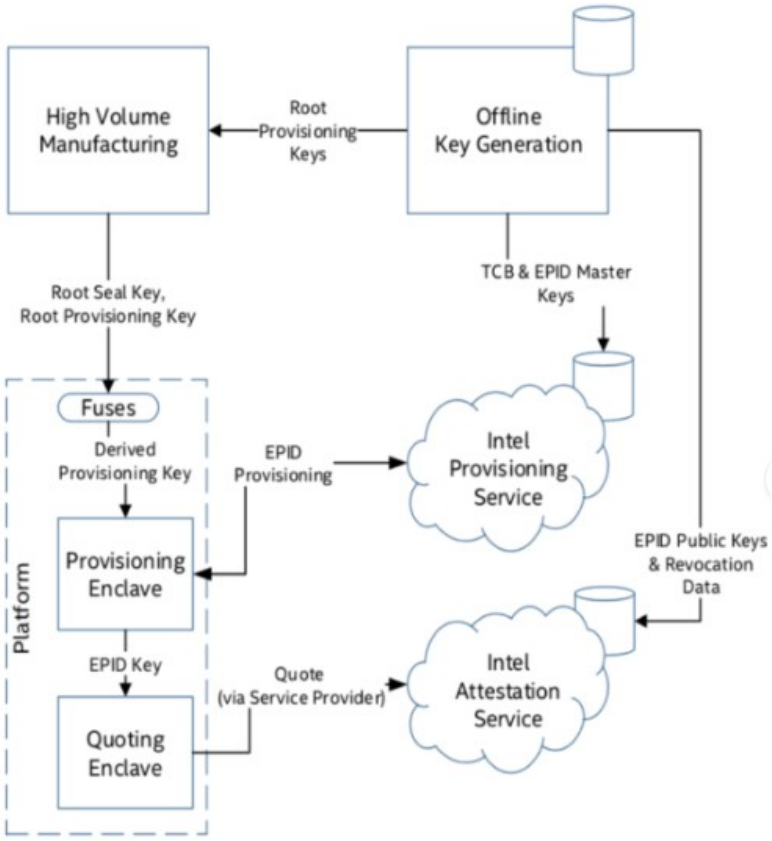

Figura 12 - Servicio Infraestructura SGX, Fuente://ibm.com

El EPID permite dividir los firmantes en grupos en función de su tipo de procesador y creando firmas con sus propias claves secretas verificables solo con la clave pública del grupo al que pertenecen. Para ello usa dos tipos de claves, la Clave de provisión (PK) que se produce en tiempo de arranque y que refleja los componentes firmware de la plataforma y la Clave de sellado de provisión (PSK) con certificados firmados por Intel.

Después de obtener la PK, la plataforma inicia el proceso de aprovisionamiento para obtener la clave de certificación usando un hash del PK que se denomina Platform Provisioning ID (PPID). El PPID determina si la plataforma se ha aprovisionado previamente.

Si ya fue provisto, se agrega la clave de certificación generada previamente demostrando que nunca fue revocada en el pasado, de lo contrario, el servidor determina el grupo de EPID y agrega los parámetros del grupo.

La clave de la plataforma junto con el certificado firmado correspondiente forman una clave privada EPID aleatoria única que se oculta matemáticamente de acuerdo con su

protocolo.

El mensaje final que completa el protocolo es enviado por el servidor que contiene el certificado de la firma[22].

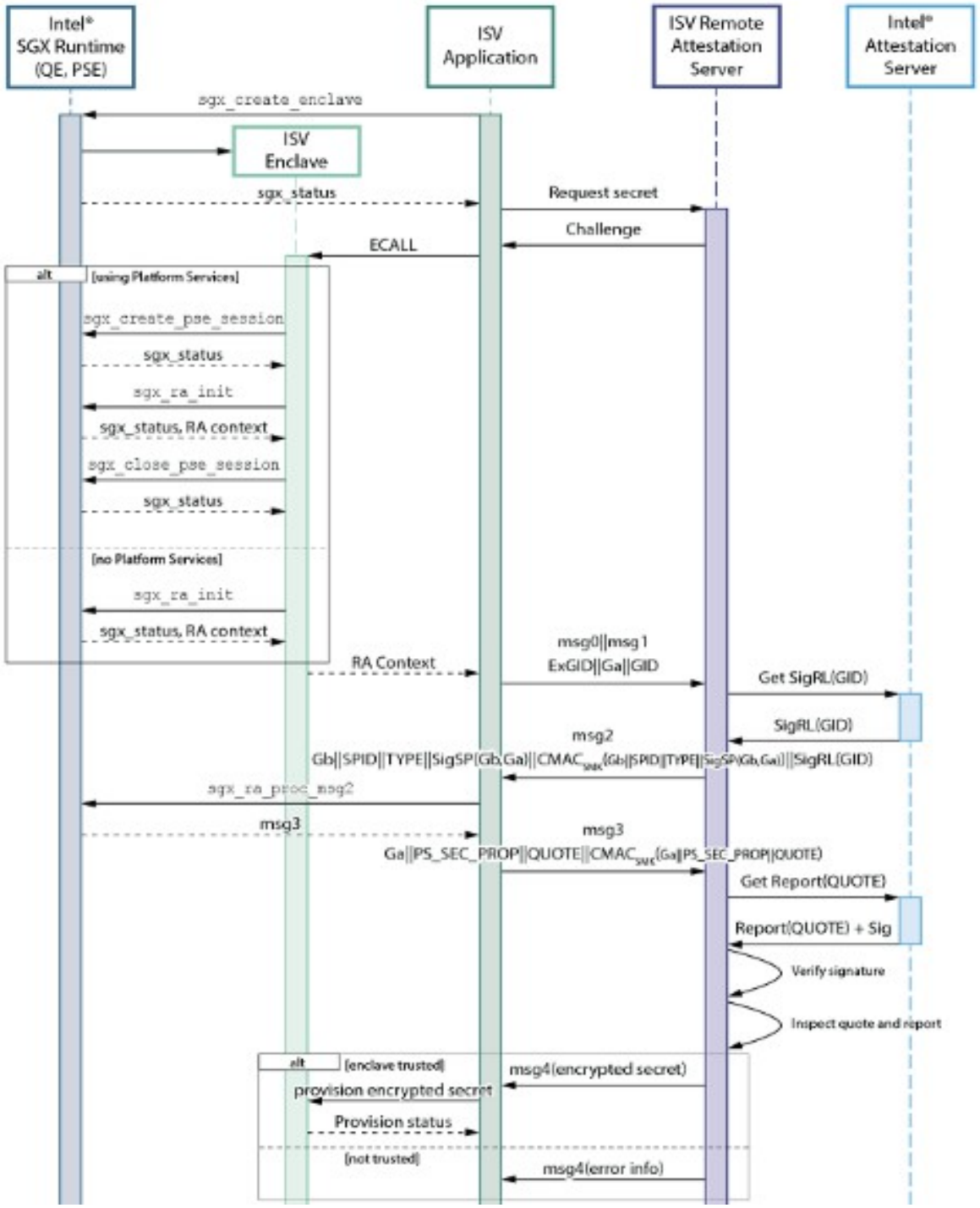

Figura 13 - Flujo comple Atestación Remota, Fuente://ibm.com

Implementación tecnológica

"En la investigación es incluso más importante el proceso que el logro mismo."
Emilio Muñoz

A continuación mostraremos los pasos realizados para la implementación del diseño mostrado en el apartado anterior. Explicaremos los procedimientos necesarios para que tengamos un dato firmado por un TEE Intel SGX y poder verificar su firma en entornos desprovistos de hardware para Intel SGX como son un SC o un programa en lenguaje Python.

Puede encontrar la implementación del código desarrollado para este proyecto en el repositorio GitHub con licencia GPLv3:

https://github.com/algovia/Contratos-Inteligentes-Sobre-Registros-Confiables-de-Polucin.git

Código C para Intel SGX

La implementación del código en lenguaje C para Intel SGX sigue el esquema de firmas desarrollado por Intel EPID, realiza la Atestación Remota y el sellado de firmas a través de algoritmo de curva elíptica. Finalmente devuelve un fichero con la firma de sellado y el dato firmado.

Se utiliza el proyecto GitHub “Intel SGX Crypto Demo” disponible en la url:

https://github.com/itsc-flensburg/Intel-SGX-Crypto-Demo

El código realiza la certificación de firmas desarrollado por Intel EPID dentro del entorno del Enclave asegurando la identidad e integridad del dispositivo Intel SGX, así como que su ejecución se realiza en su última versión de firmware y adquiriendo como resultado una clave que puede ser usada para firmar mensajes.

El trabajo realizado modifica este código para transformar las claves devueltas por el proceso de Atestación Remota desde el formato Big Endian, aquel que ordena los bytes del más significativo al menos significativo, a Little Endian, formato que manejan las firmas de Ethereum, adaptando así el datagrama que devuelve el TEE al formato entendible por la Blockchain.

Dentro del propio Enclave, zona segura de memoria del TEE, se simulan las llamadas a los sensores para la adquisición de datos y cálculo de emisiones.

El dato simulado es firmado con las firmas entregadas por la Atestación Remota, devolviendo un fichero de texto con el certificado de firmas y el dato firmado.

Código Solidity para Smart Contracts en Blockchain de Ethereum

Se decide usar las redes Blockchain de Ethereum y el uso del lenguaje Solidity para la implementación de Smart Contracts con el código necesario para comprobar la integridad y validez del dato firmado. La identidad usada para esta firma puede verificarse a través de la atestación remota, como se explica en la siguiente subsección,demostrando que no ha sido una clave inventada sino creada a través del proceso de Atestación Remota de Intel.

En un primer paso desplegamos el Smart Contract para comprobación de claves por curva elíptica en el Ethereum IDE Remix. Debido al coste del proceso es necesario cambiar el entorno de JavaScript VM a Web3 Provider, utilizando ganache-cli como proveedor del servicio.

La verificación de la firma del mensaje demuestra la integridad del mismo quedando el dato a disposición de cualquier usuario al ser grabado mediante transacción en la Blockchain.

Este trabajo utiliza el proyecto GitHub “Elliptic Curve Solidity” disponible en la url:

https://github.com/tdrerup/elliptic-curve-solidity

Los cambios previos en el código Intel SGX para transformar las claves de Big Endian a Little Endian sirven para disponer de los datos formados en el formato que el SC pueda entender, permitiendo así realizar los cálculos necesarios para comprobar el firmado de claves por algoritmo de curva elíptica.

De esta forma, en un segundo paso, el usuario puede comprobar en el SC que la firma de claves es correcta y disponer del dato firmado sabiendo que proviene de un TEE que asegura su identidad e integridad por Atestación Remota.

El contrato con los cambios desarrollados para verificar la firma y guardar el dato en la Blockchain se encuentra desplegado en Rinkeby Tesnet Network y se puede consultar el mismo desde:

https://rinkeby.etherscan.io/address/0xecf36a257f996b9e56dee18f826112402f9f77b6

El contrato se encuentra desplegado en la siguiente dirección donde cualquier usuario podrá consultar las transacciones realizadas y llamar a las mismas.

0Xecf36a257f996b9e56dee18f826112402f9f77b6

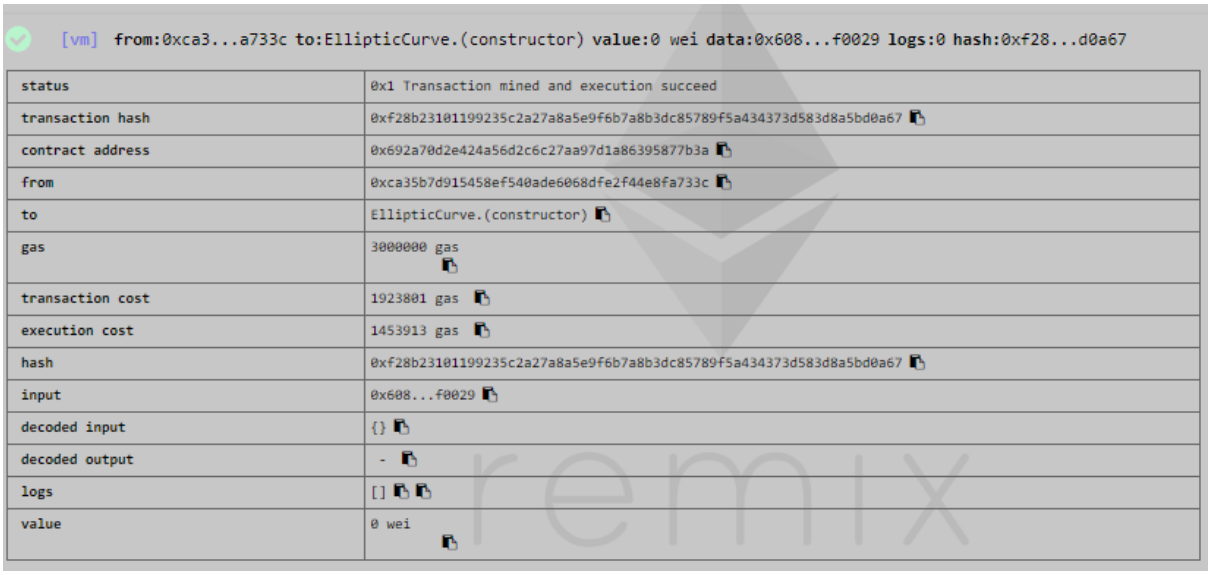

Figura 14 - Resumen transacción despliegue Smart Contract

Al desplegar el Smart Contrat en la Blockchain podemos observar en su resumen, que la transacción se ha realizado correctamente, devolviendonos su Hash y la dirección del contrato. Además podemos ver que el coste de la transacción ha sido de 1.923.801 gas. Una vez que se ha desplegado el SC podemos usar los métodos de los que dispone.

Verificación de firma en ausencia de hardware específico Intel SGX

Como ya hemos presentado, IBM da la posibilidad de verificar el certificado de firma de sus dispositivos SGX de manera remota, a través de su Atestación Remota, enfrentando el certificando a sus servidores y devolviendo una respuesta a la verificación.
Aunque lo que realmente resulta interesante es que no es necesario disponer de hardware específico Intel SGX para poder realizar la comprobación del certificado de claves generado en el TEE Intel SGX.

En el código Solidity desarrollado para el SC en la Blockchain de Ethereum ya se realizó esta comprobación sin necesidad de este hardware específico. Aunque existen otras formas de conseguir atestiguar el dato en otro tipo de plataformas.

Para ello se ha utilizado verificación a través de código Python con parámetros generados por la librería python-ecdsa, demostrando que no es necesario tener hardware Intel SGX para atestiguar la validez de las firmas.

Se utiliza el proyecto GitLab “Sign and verify with python-ecdsa” disponible en la url:

https://gitlab.com/snippets/1855863

En el código podemos apreciar como el proceso de verificación hace uso de la clave pública y la firma para atestiguar la veracidad de la firma y demostrar que proviene de un TEE válido. Como salida disponemos del Hash del mensaje y la firma del dato. La firma del dato viene representada por los valores ‘r’ y ‘s’ y su clave pública en los valores ‘x’ e

‘y’, valores que permiten representar punto en el algoritmo de la curva elíptica y verificar su validez.

Pruebas y análisis de resultados

"Any sufficiently advanced technology
is indistinguishable from magic."
Arthur C Clarke

El presente apartado explora el análisis de costes en el despliegue y ejecución del Smart Contract en Ethereum, así como la viabilidad tecnológica de la propuesta mostrando los pasos necesarios para su ejecución.

Análisis de costes 'gas' Ethereum

El gas es la unidad de medición del coste computacional al ejecutar transacciones o desplegar contratos inteligentes en la red Etereum. El uso de gas se ve reflejado como la cantidad de Ether que se va a pagar por coste computacional al desplegar o ejecutar métodos del SC en la Blockchain.

En el desarrollo de la prueba de viabilidad con el código que se ha desarrollado hemos podido recoger los costes que suponen el despliegue del Smart Contract en la red, la verificación de la firma del SC y el coste por almacenar el dato.

Coste por despliegue de contrato

Hemos podido comprobar como el coste medio en gas en el despliegue del Smart Contract ha sido de 1.967.700 unidades de gas lo equivalente a 1'6 $ o unos 1'4 € al precio actual del gas (1.2 x 10-18 Ether) y el Ether (aproximadamente 269 $ o 239 €).

Un coste tan elevado denota que el Smart Contract es demasiado largo, lo que puede suponer un uso indebido de la Blockchain, pudiendo llegar a colapsar y hacerla inviable. Esta posibilidad se ve reducida al establecer un coste máximo por gas para las transacciones pero aún así es excesivo.

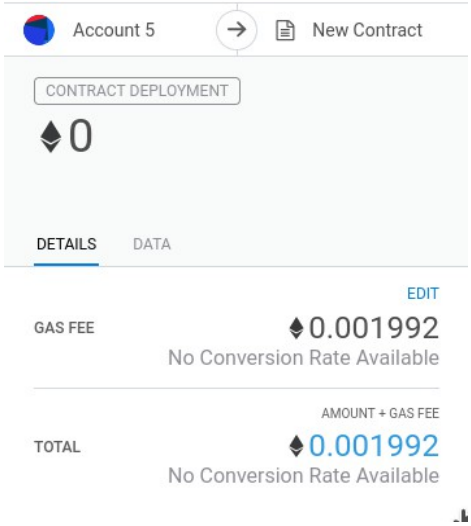

Figura 15 - Coste en gas por despliegue del contrato

Coste por verificación de firma

En el caso del coste a la hora de evaluar la validez de la firma se ve reducido a 0 unidades de gas. Esto se debe a que las funciones denominadas puras en un Smart Contract no conllevan coste de transacción. Lo que resulta verdaderamente ventajoso, ya que cualquier usuario podrá validar la firma de manera gratuita, pudiendo ser usado por otros contratos sin coste adicional.

La web https://ethgastable.info/ indica que el coste de la función de verificación de firma de Ethereum ECRECOVER es de 3000 gas unos 0’002 $, por lo que en comparación con nuestra comprobación de firma de Intel SGX parece una solución razonable.

Coste por guardado de datos

El coste de gas se ve reflejado en el trabajo computacional que el SC debe hacer, cómo máximo una transferencia ETH estándar requiere un límite de 21.000 unidades de gas, unos 0´0017 dólares. En nuestro caso el coste por almacenar el dato es de 1267271 unidades de gas, lo que sería 1,4 $ al precio actual del gas (1.2 x 10-18 Ether) y el Ether (aproximadamente 269 $ o 239 €).

En nuestro caso el coste de verificación de firma es cero, pero al guardar el dato en la Blockchain no estamos utilizando una función pura. Este coste es único y constante para cada dato guardado, ya que solo se guarda una vez por dato. Además el dato sólo será guardado en caso de superar la validación de la firma ques es gratuita. después de haber superado

El código desplegado sirve para verificar la firma del dato sin necesidad de gastar ningún ether y con un coste único para los datos que queden grabados en la blockchain.

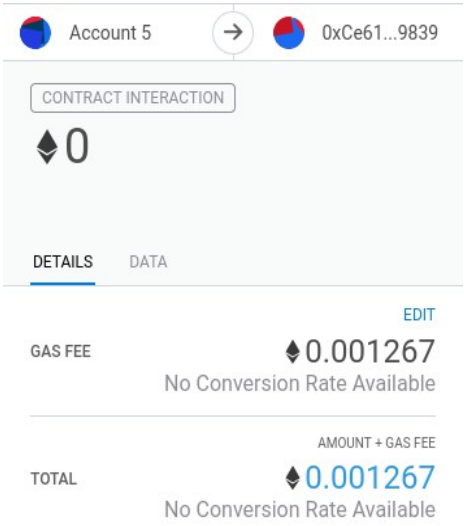

Figura 16 - Coste en gas por guardado de datos en Blockchain

En vista de los costes analizados y sabiendo que el precio del ether en la red fluctúa, podemos determinar que actualmente sería viable su implantación. Ya que el mayor coste se encuentra en la creación del contrato, el dato solo se guarda en caso de superar la validación de la firma y la transacción es única ya que solo se paga una vez por cada dato a guardar.

Análisis de viabilidad

A continuación procedemos, mediante el código implementado y explicado en la sección anterior, a realizar una prueba de viabilidad del sistema. Para ello mostraremos los pasos necesarios para mediante el uso del código desarrollado alcanzar los objetivos funcionales del mismo.

Puede encontrar la implementación del código desarrollado para este proyecto en el repositorio GitHub con licencia GPLv3:

https://github.com/algovia/Contratos-Inteligentes-Sobre-Registros-Confiables-de-Polucin.git

Obtención de dato firmado

En un primer paso ejecutaremos el código desarrollado para el Intel SGX que nos dará como respuesta el dato firmado. Recordamos que el formato de las firmas fue modificado para ser devuelto en Little Endian, ya que es el formato que maneja los SC en Ethereum.

El contenido del fichero resultado muestra en su primera la línea el dato simulado por un sensor en un TEE firmado criptográficamente. En la segunda y tercera podemos observar los valores para firma del dato ‘r’ y ‘s’. En la últimas líneas vemos los ‘x’ e ‘y’ como valores de la clave pública. Que sirven para verificar la firma mediante cálculo en el algoritmo de curva elíptica. [1]

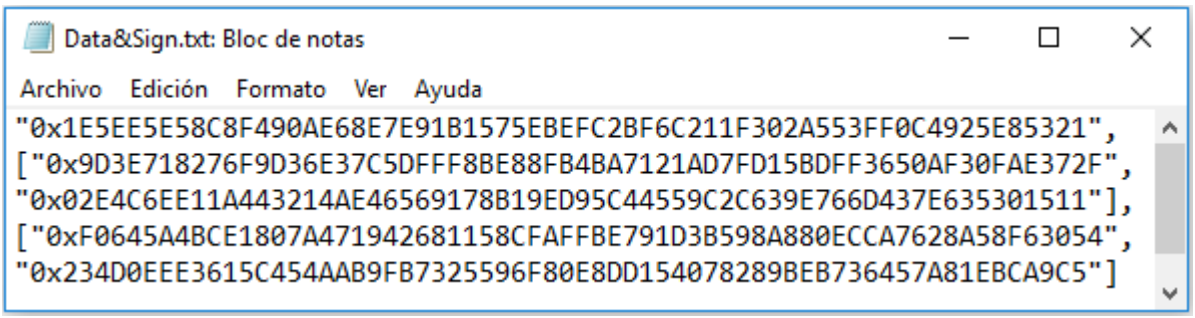

Figura 17 - Fichero de salida Intel SGX

1 La firma se representa por ‘x’, ‘y’, ‘r’ y ‘s’ porque representan puntos en la curva elíptica del algoritmo utilizado

Verificar la firma del dato

Verificación mediante Smart Contract

Tomamos el contenido del fichero generado al ejecutar el código para SGX y proveemos sus datos el método “validateAndRecordMessage”[2] del SC.Este método permite demostrar la validez de la firma entregada por Intel SGX sin necesidad de disponer de hardware de Intel.

Figura 18 - Despliegue Smart Contract

Como resultado de la ejecución del contrato recibimos el Hash de la transacción y un valor de salida (decoded output) con valor true. Los datos usados en la transacción quedan registrados en la Blockchain, pudiendo ser consultados en el resumen de la transacción identificado por su código hash. Además, queda registrado que la verificación de la firma ha sido satisfactoria.

2 Se introducen los valores ‘x’, ‘y’, ‘r’ y ‘s’ como puntos de la curva elíptica

[call] from:0x4d69d7a62c98cf0681e7d8d7f5f86245983217a8
to:EllipticCurve.validateSignature(bytes32,uint256[2],uint256[2]) data:0x04e...ca9c5

transaction hash	call0x4d69d7a62c98cf0681e7d8d7f5f86245983217a80xf819fa49eef73f82ecbe3925f6a6d9333c70821f0x04e960d71e5ee5e58c8f490ae68e7e91b1575ebefc2bf6c211f302a553ff0c4925e853219d3e718276f9d36e37c5dfff8be88fb4ba7121ad7fd15bdff3650af30fae372f02e4c6ee11a443214ae46569178b19ed95c44559c2c639e766d437e635301511f0645a4bce1807a471942681158cfaffbe791d3b598a880ecca7628a58f63054234d0eee3615c454aab9fb7325596f80e8dd154078289beb736457a81ebca9c5
from	0x4d69d7a62c98cf0681e7d8d7f5f86245983217a8
to	EllipticCurve.validateSignature(bytes32,uint256[2],uint256[2]) 0xf819fa49eef73f82ecbe3925f6a6d9333c70821f
hash	call0x4d69d7a62c98cf0681e7d8d7f5f86245983217a80xf819fa49eef73f82ecbe3925f6a6d9333c70821f0x04e960d71e5ee5e58c8f490ae68e7e91b1575ebefc2bf6c211f302a553ff0c4925e853219d3e718276f9d36e37c5dfff8be88fb4ba7121ad7fd15bdff3650af30fae372f02e4c6ee11a443214ae46569178b19ed95c44559c2c639e766d437e635301511f0645a4bce1807a471942681158cfaffbe791d3b598a880ecca7628a58f63054234d0eee3615c454aab9fb7325596f80e8dd154078289beb736457a81ebca9c5
input	0x04e...ca9c5
decoded input	{ "bytes32 message": "0x1e5ee5e58c8f490ae68e7e91b1575ebefc2bf6c211f302a553ff0c4925e85321", "uint256[2] rs": ["71123445160248959697696282409987356953249309945002445653641897709467522185007", "130883979203785823641913832868293491063574647201918188829770087253192422734 5"], "uint256[2] Q": ["108732391567333200221457625963927767977695479562207758445897784640462998876244", "159670999710142391765370011089110979868482279634531046556632865049688615592 37"] }
decoded output	{ "0": "bool: true" }
logs	[]

Figura 19 - Resumen transacción verificación firma Smart Contract

Podemos apreciar en el resumen de la transacción como el método de validación de firma no conlleva un coste por transacción al tratarse de una función pura de Solidity.

Sin embargo, en el caso del método validateAndRecordMessage, el hecho de almacenar el dato en la Blockchain y no tratarse de una función pura supone un coste de 1.267.221 unidades de gas.

Figura 20 - Resumen transacción verificación firma y guardado de dato del Smart Contract

Verificación mediante código Python

La prueba anterior demuestra como un dato proveniente de un sensor, bajo la Atestación Remota y firmado por un TEE Intel SGX, puede ser verificado en un Smart Contract desplegado en la Blockchain de Ethereum y puesto a disposición del usuario sin intervención de terceros.
Finalmente utilizaremos otro modo de verificar la firma mediante código Python mediante la librería python-ecdsa.

```
#!/usr/bin/python3

import ecdsa
from hashlib import sha256

message = b'468'

# We hash "message" string into sha256
hash = sha256(message).hexdigest()

public_key =
'EE489B009194DC973D089738873FB7BD17B3673FB0596EBAAE7A36D6032CECEE98921068420DE70A978B2212DE6D3B0ECCC342F5CB42FD5C8E8B8F621DAADBE0'

sig =
'A5302D9ACF44184BCC017B0FC31BAE1A4EDA20A133D3447CB02C5E8DB19D688BCE5209E91170AB9E449A09BDB5C46E857685B7C5E8DC01E5AD3C62CDB41DC9A6'

vk = ecdsa.VerifyingKey.from_string(bytes.fromhex(public_key), curve=ecdsa.NIST256p)
```

```
isCorrect = vk.verify(bytes.fromhex(sig), message, hashfunc=sha256)

print('Is a valid key?: ' + str(isCorrect))

x = public_key[:64]
y = public_key[64:]
r = sig[:64]
s = sig[64:]

print('"0x%s", ["0x%s", "0x%s"], ["0x%s", "0x%s"]'%(hash, r, s, x, y))
```

Como podemos ver se asignan los valores del fichero de salida de Intel SGX para la clave pública y su firma a las variables ‘public_key’ y ‘sig’ del programa. La biblioteca python-ecdsa realiza el cálculo de los puntos de la curva para atestiguar que forman parte de ella y así determinar qué se trata de una clave y una firma válidas.

Cumpliendo con las especificaciones del prototipo se desarrolla la prueba de concepto con resultado exitoso procedemos a realizar el análisis de estos resultados obtenidos.

Conclusiones

"Just because something doesn't do what you planned it to do doesn't mean it's useless."
Thomas Edison

Para determinar el grado de cumplimiento de los objetivos propuestos en este proyecto y después de explicar las bases teóricas de la investigación y las posibles aplicaciones prácticas que pueda tener, podemos formular de forma clara y detallada de donde nacen nuestras conclusiones y para qué sirven.

Actualmente ya podemos encontrar organizaciones y herramientas que permiten a la Blockchain interactuar con el mundo real; en nuestro caso, la sensorización de un barco. El uso de estas herramientas y organizaciones, pese a legislación y los contratos de privacidad, supone la cesión de información a un intermediario, lo que implica tener que ceder la confianza a un tercero.

Lo interesante de nuestro estudio es el hecho de no tener que ceder esa confianza, conectando directamente los sensores a un TEE ofreciendo a la Blockchain un registro confiable de dato, verificando en la Blockchain la integridad de los mismos. Hemos desarrollado una prueba de concepto funcional. Sin embargo, la estimación de costes no es la más ajustada o reducida. Sería necesario el uso de otro algoritmo de firma más económico en la blockchain de Ethereum, como el que ya usa para la gestión de sus identidades, para reducir drásticamente estos costes.

La aplicación de esta tecnología, que asegura la legitimidad del dato y su libre disposición sin ceder la confianza en terceros, crea un ecosistema de Smart Contracts que permite irrumpir en el ciclo productivo de cualquier sector. Permitiendo acordar cláusulas por las partes implicadas en un Smart Contract, que son de obligado cumplimiento y cuya autoejecución depende de un dato firmado por un TEE no dependiente de terceros.

Planteamiento de trabajos futuros

"Just because something doesn't do what you planned it to do doesn't mean it's useless."
Thomas Edison

A continuación, se presentan algunos trabajos futuros que pueden desarrollarse como resultado de esta investigación o que, por exceder el alcance de esta tesis, no han podido ser tratados con la suficiente profundidad. Además, se sugieren algunos desarrollos específicos para apoyar y mejorar el modelo y metodología propuestos.
Estas líneas pueden servir para retomarlas posteriormente o como opción a trabajos futuros a otros investigadores.

1. Bajar el nivel de coste de gas por verificación de firmado de claves
Exploración de atestación del dato mediante algoritmos de creación de claves más económicos y eficaces que permitan reducir los costes de ejecución del las peticiones realizadas por los Smart Contracts permitiendo un mayor número de consultas a menor coste. En este sentido, utilizar el algoritmo de firma usado por Ethereum desde el entorno de ejecución segura, reduciría significativamente los costes.

2. Desarrollar aplicaciones que hagan uso de esta información
Codificación de Smart Contracts que permitan hacer uso de estos datos modelando casos de usos diferentes, como sanciones administrativas en caso de caso de detectar anomalías o fraudes y su portabilidad a otros sistemas y mercados de polución como puede ser el transporte aéreo, el transporte por carretera, la industria o las centrales termoeléctricas por ejemplo.

3. Diseño hardware detallado del dispositivo a utilizar
Diseño detallado del desarrollo industrial necesario para fabricar el dispositivo y que eviten la manipulación física del mismo permitiendo intervenir en la cadena de seguridad necesaria a la hora de atestiguar la autenticidad de los datos generados.

Introduction

> “Let them riso to the challenge of Sustainable Development Goals and act,
> not out of self interest, but out of common interest
> .I am very aware of the preciousness of time. Seize the moment, act now.”
> Stephen Hawking

Air pollution has become one of the main problems in Climate Change for the generation of Greenhouse Gases (GHG) due to the burning of fossil fuels by man.
Currently we do not have mechanisms that allow us to know, in real time, the amount of Carbon Dioxide (CO2) that emitted into the atmosphere any Emission Source such as thermoelectric plants, industry or means of transport such as maritime, considered one of the main sources of CO2 emissions.

This work proposes the use of Secure Devices in the Internet of Things that allow to measure these emissions in real time; and the generation of trust by connecting the data generated in Secure Execution Environments (TEE) to an immutable record in the Blockchain, which guarantees that the data is stored, processed and protected in an isolated and reliable environment; allowing the creation of an ecosystem of applications that helps regulate pollution and boost an economy more focused on the ecological footprint than on the economic benefit.

This project shares the spirit and motivations of the GRASIA research group and its P2P Models project in the construction of decentralized and democratic organizations using Blockchain technology, in order to promote a new type of sustainable collaborative economy. Likewise, the work is in tune with the Sustainable Development Goals (SDG) of the United Nations (UN).

The use of Blockchain and Smart Contracts networks provides desirable characteristics, such as the decentralization of infrastructure or the ability to create immutable and transparent records. However, it has important challenges, such as the inability to obtain data external to the Blockchain, for which Oracles are traditionally used. The Oracles, as opposed to the Blockchain spirit, are usually provided by private companies, such as the SmartContract company (not to be confused with the Smart Contracts concept) that pretends to be an Oracle between the conventional banking and the Blockchain or the Oraclize company that creates connections between the Blockchain and Web API's or Dapps, losing the capacity of decentralization and transparency to be maintained by a single centralized entity and not be supported and supervised by its contributors.

In the line of creation of decentralized Oracles we can find ChainLink that tries to create the first network of Oracles that allows Smart Contracts to connect to external data feeds, as well as to APIs or payment systems; or the Town-Crier project of Ari Jules, an Oracle that takes advantage of the power of the Intel SGX TEE to guarantee the origin and integrity of code execution that allows interacting with Smart Contracts.

For this reason we propose the creation of Oracles that do not depend on trusting third parties. That allow the acquisition of real world data through Secure Devices in the Internet of Things (IoT), without the need to give our trust to any body or organization and allowing any actor interested in this information to verify the authenticity of the generated data and make use of them.

Conclusions

"Just because something doesn't do what you planned it to do doesn't mean it's useless."
Thomas Edison

To determine compliance with the objectives proposed in this project and after explaining the theoretical bases of the research and the possible practical applications that may have, we can formulate in a clear and detailed manner where our conclusions are born and what they are for.

Currently we can find organizations and tools that allow the Blockchain to interact with the real world; in our case, the sensorization of a ship. The use of these tools and organizations, despite legislation and privacy contracts, involves the transfer of information to an intermediary, which implies having to assign confidence to a third party.

The interesting thing about our study is the fact that we do not have to give up that trust, directly connecting the sensors to a TEE offering the Blockchain a reliable data record, verifying in Blockchain the integrity of the same. We have developed a functional proof of concept. However, the cost estimate is not the most adjusted or reduced. It would be necessary to use another more economical signature algorithm in the Ethereum blockchain, such as the one you already use for the management of your identity, to drastically reduce these costs.

The application of this technology, which ensures the legitimacy of the data and its free disposal without losing confidence in third parties, creates an ecosystem of Smart Contracts that allows breaking into the productive cycle of any sector. Allowing to agree clauses by the parties involved in a Smart Contract, which are mandatory and whose self-execution depends on a data signed by a TEE not dependent on third parties.

Bibliografía

[1] Grupo de Investigación GRASIA - P2P Models. Retrieved from https://p2pmodels.eu/

[2] G. Assembly (2014). Sustainable Development goals Improving human and planetary wellbeing. Retrieved from https://www.undp.org/content/undp/es/home/sustainable-development-goals.html

[3] Satoshi Nakamoto (October 31, 2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

[4] Don Tapscott, Alex Tapscott (2016). Ed. Deusto. Grupo Planeta. La Revolución Blockchain. Retrieved from www.planetadelibros.com Título original: Blockchain Revolution. Ed. Portfolio (2016)

[5] Nick Szabo (1 Sept 1997). First Monday. Peer-Review Journal on the Internet. Formalizing and Securing Relationships on Public Networks. Retrieving from https://firstmonday.ort

[6] academy by Bit2me - Smart Contracts: ¿Qué son, cómo funcionan y qué aportan?. Retrieved from https://academy.bit2me.com/que-son-los-smart-contracts/

[7] Jon Buck(18 Octubre 2017). Cointelegraph.com. Oráculos de Blockchain, explicados. Retrieved from https://es.cointelegraph.com/explained/blockchain-oracles-explained

[8] J. Slobodník (Feb 2, 2018). Medium Corporation. How Oracles connect Smart Contracts to the real world. Retrieved from https://medium.com/bethereum/how-oracles-connect-smart-contracts-to-the-real-world-a56d3ed6a507

[9] Ian Lucas Diaz (Mayo 2018). IOTA Hispano. Oráculos: Conectando el mundo real con los Smart Contracts. Retrieved from https://iotahispano.com/2018/05/16/oraculos-conectando-el-mundo-real-con-los-smart-contracts/

[10] P. Jain, S.Desai, S. Kim, M. Shih, J. Lee, C. Choi, Y. Shin, T. Kim, B. Byunghoon Kang, D. Han (2017). OpenSGX: An Open Platform for SGX Research. Retrieving from https://www.researchgate.net/publication/298435049

[11] Global Platform Inc. (2018) Global Platform. An Introduction To The Trusted Execution Environment For Mobile Services Security. Retrieved from https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Trusted-Execution-Environment-15May2018.pdf

[12]IThink UPC - Recomendaciones de seguridad para dispositivos IoT Retrieving for https://www.ithinkupc.com/es/blog/recomendaciones-de-seguridad-en-dispositivos-iot

[13] Cheng, R., Zhang, F., Kos, J., He, W., Hynes, N., Johnson, N., … Song, D. (2018). Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution. Retrieved from http://arxiv.org/abs/1804.05141

[14] Nieves Cruz Felipe. (2006, octubre 1). La investigación exploratoria. Retrieving for https://www.gestiopolis.com/la-investigacion-exploratoria/

[15] C. Martinez (2018).- Investigación descriptiva: Tipos y características. Retrieved from https://www.lifeder.com/investigacion-descriptiva/

[16] K. Beck, J. Grenning, R.C. Martin, M. Beedle, J. Highshith, S. Mellor, A. van Bennekum, A. Hunt, K. Schwaber, A. Cockburn, R. Jeffries, J. Sutherland, W. Cunningham, J. Kern, D. Thomas, M. Fowler, B. Marick (2001). Manifesto for Agile Software Development. Retrieving from https://agilemanifesto.org/

[17] Liken Carbon Hub - Climate Change Advisors. Retrieved from http://www.likencarbon.com/

[18] Wedge Global - wave energy Retrieved from https://vimeo.com/212557660

[19] Leo Hickman (2 May 2017). Carbon Brief. On the evening of Tuesday, 8 December, 1981, the UK's only commercial TV channel, ITV, broadcast an hour-long documentary called "Warming Warning". Retrieved from https://www.carbonbrief.org/warming-warning-1981-tv-documentary-warned-climate-change

[20] Organización Meteorológica Mundial (2010). OMM-Nº1119. El estado del clima mundial 2001 – 2010. Un decenio de fenómenos climáticos extremos. Retrieving from https://library.wmo.int/pmb_ged/wmo_1119_es.pdf

[21] Vergés-Jaime, J. (2009). El Protocolo de Kyoto, y el "mercado de derechos de emisión" de CO2. Retrieved from https://ddd.uab.cat/pub/estudis/2009/hdl_2072_43191/ieakyoto.pdf

[22] Intel Software (July 4, 2018). Intel Software Guard Extensions. Code Sample: Intel® Software Guard Extensions Remote Attestation End-to-End Example Retrieving from https.://software.intel.com/en-us/articles/code-sample-intel-software-guard-extensions-remote-attestation-end-to-end-example

Glosario

Contratos inteligentes / Smarts Contracts
: Programa informático que facilita, asegura, hace cumplir y ejecuta acuerdos registrados entre dos o más partes.

Cadenas de bloques / Blockchain
: Estructura de datos en la que la información contenida se agrupa en conjuntos a los que se les añade metainformación relativa al bloque de la cadena anterior.

Cadenas de suministro de alta calidad
: Llevar a cabo en la cadena de procesos de una organización acciones para conseguir que sea eficaz, competitiva y ecológica.

Clave de sellado
: Conjunto de firmas digitales y sellado de tiempo.

Atestación remota
: Entidad que gana la confianza de un proveedor o productor remoto de algún tipo.

Internet de las Cosas
: Concepto que se refiere a una interconexión digital de objetos cotidianos con internet.

Web API's
: Interfaz de programación de aplicaciones como conjunto de rutinas que provee acceso a funciones de un determinado software.

Dapps
: Acrónimo en referencia de Aplicaciones Descentralizadas.